

# Hardening Moodle

Concept and Realization of a Security  
Component in Moodle

a project by

Andreas Gigli, Lars-Olof Krause,  
Björn Ludwig, Kai Neumann, Lars  
Schmidt and Melanie Schwenk



FACHHOCHSCHULE

**GIESSEN**

**FRIEDBERG**

UNIVERSITY OF APPLIED SCIENCES



# Agenda

- Plugin Installation in Moodle
- Intrusion Detection System / Intrusion Prevention System
  - Integration of PHP-IDS/IPS-System
  - Administration of PHP-IDS/IPS-System
  - Statistics of PHP-IDS/IPS-System
- Tests with Apache JMeter
- Suhosin
  - Administration of Suhosin-System
  - Statistics of Suhosin-System
- OWASP Top 10



# Plugin Installation in Moodle



# Plugin installation

- Administrations are created as local plugin
- IDS/IPS-System is inside the local plugin folder
- Installation by copying folder into the local folder of moodle
- Database-Tables are created by moodle using an DBXML-File
- Standard Database-Entrys are added automatically
- User is ask to set some access rights & change of one corefile



# Intrusion Detection System/ Intrusion Prevention System

- Integration of PHP-IDS/IPS-System
- Administration of PHP-IDS/IPS-System
- Statistics of PHP-IDS/IPS-System



# Integration of PHP-IDS/IPS-System

- Automatic installation as described before
- Configuration is stored in database  
→ Cluster-ready
- Modification of only one moodle-internal file is needed to get IDS-/IPS system running
- New filters and converter are stored in moodledata folder  
→ Each single node of the cluster downloads the files to its own installation folder to save traffic



# Intrusion Prevention System

- Evaluates given impact from IDS
- Evaluates Total and Global impact
- Is able to prevent the user from performing further malicious requests



# Reactions on attacks (I)

- Log attack (Default impact 5)
  - Logs the attack in a database
- Warn user (Default impact 10)
  - Cancels the script with the attacking vector
  - Warns the attacker by showing the actions performed against the attacking user





# Reactions on attacks (II)

## Error: Malicious request

Navigation



[Home](#)

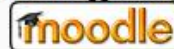
An attempt to inject malicious code into the system has been detected. For security reasons your request has been stopped.

The problem was logged to our database.

The system administrator has been informed about this issue.

Your account has been temporarily disabled. Please contact your system administrator to request re-activation.

You are not logged in. ([Login](#))





# Reactions on attacks (III)

- Kick user (Default impact 30)
  - Kicks user by terminating his session id
  - Requires a captcha on attackers next login
- Admin mail (Default impact 45)
  - Sends an email containing the log of the attack to the admins
- Ban user (Default impact 50)
  - The account of the attacker gets banned and must be re-activated via the admin interface



# Total and Global Impact

- Evaluates Total Impact
  - Total Impact of one user in a defined time
  - If the Total Impact exceeds defined values the same reactions as on normal impact can be taken
- Evaluates Global Impact
  - Impact of all users in a defined time
  - If the Global Impact exceeds a defined value a mail to the administrator is sent



# Administration of PHP-IDS/IPS-System (I)

Home ► Site administration ► IDS/IPS ► Administration

**Navigation**

- Home
  - My home
  - Site pages
  - My profile

**Settings**

- My profile settings
- Site administration
  - Notifications
  - Registration
  - Advanced features
    - Users
    - Courses
    - Grades
    - Location
    - Language
    - Plugins
    - Security
    - Appearance
    - Front page
    - Server
    - Reports
    - Development
  - IDS/IPS
    - Administration**
    - Logs
    - Banlist
  - Suhosin

## IDS / IPS Administration

**Updates**

[Search for new PHP-IDS-Data](#)

**IDS/IPS System**

IDS system is running

Active ☒

User ID of Super AdminRequired field 2

**Caching**

Cache TypeRequired field session

Expiration timeRequired field 600

**Threshold**

LogRequired field 12

Admin E-mailRequired field 80

Kick UserRequired field 40

Ban UserRequired field 100

WarnRequired field 9



# Administration of PHP-IDS/IPS-System (II)

- The IDS/IPS-Administration is included as own menu entry
- Administration contains
  - Search for new PHP-IDS default\_filter.xml and Converter.php
  - Autoupdate for the new files from PHP-IDS
  - Activate/Deactivate System
  - Selected Superadmin which is not monitored by the System
  - Caching-Types
  - Threshold-Configuration
  - Admin-Mail-Configuration



# Administration of PHP-IDS/IPS-System (III)

- Banlist contains
  - List of banned users
  - Ability to view the user's profile
  - Total Impact of the banned users
  - Button to unban users



# Statistics of PHP-IDS/IPS-System (I)

[Home](#) ► [Site administration](#) ► [IDS/IPS](#) ► [Logs](#)

Navigation

[Home](#)

- My home
- Site pages
- My profile

Settings

[My profile settings](#)

- Site administration
  - Notifications
  - Registration
  - Advanced features
    - Users
    - Courses
    - Grades
    - Location
    - Language
    - Plugins
    - Security
    - Appearance
    - Front page
    - Server
    - Reports
    - Development
  - IDS/IPS
    - Administration
    - Logs
    - Banlist
  - Suhosin

IDS / IPS Statistics

[Total Impact per Day \(1 month\)](#)  
[Total Impact per Hour \(1 month\)](#)  
[Count of Attacks \(1 month\)](#)  
[Count of Actions per Weekday \(1 month\)](#)  
[Top-10-Hacker](#)  
[Top-10-Targets](#)

Top-10-Targets

You can see the "top 10" targets.

| Files/Courses                         | Actions in the past month |
|---------------------------------------|---------------------------|
| /moodle/local/idsadmin/logs_graph.php | 680                       |
| /moodle/local/idsadmin/logs.php       | 640                       |
| /moodle20/admin/search.php            | 494                       |
| /moodle/local/idsadmin/logs_table.php | 96                        |
|                                       | 32                        |
| /moodle/theme/image.php               | 8                         |



# Statistics of PHP-IDS/IPS-Sytem (II)

- Component consists of 3 files:
  - **Logs.php**
    - Shows an overview of the possible graphs and tables
    - Loads the graphs from logs\_graph.php and the tables from logs\_table.php
  - **Logs\_graph.php**
    - With the help of the Moodle data graphlib.php the graphs for the analysis are created
    - Gets the needed data from the database „mdl\_intrusions“
  - **Logs\_table.php**
    - Implements a function which returns a HTML-String with the chosen Table
    - Gets the needed data from the database „mds\_intrusions“





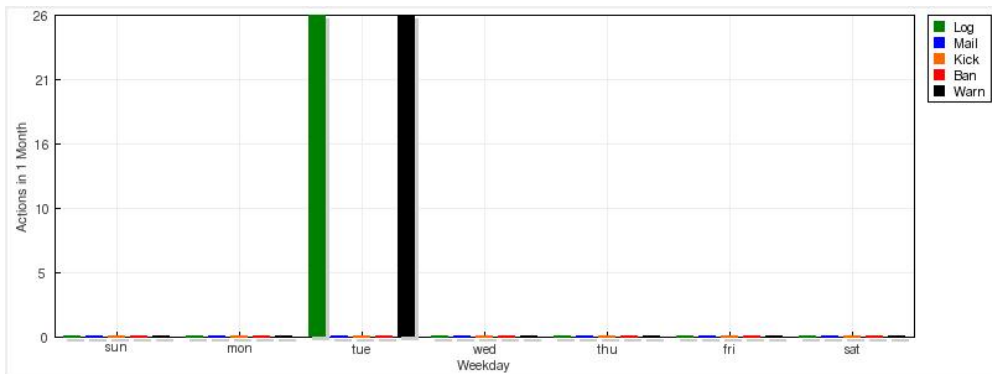
# Analysis

- The basis for the analysis is 1 month (30 days)
- Analysis as following options:
  - Total Impact per Day (1 month)
  - Total Impact per Hour (1 month)
  - Count of Attacks (1 month)
  - Count of Actions per Weekday (1 month)
  - Top-10-Hacker
  - Top-10-Targets



# Analysis Examples

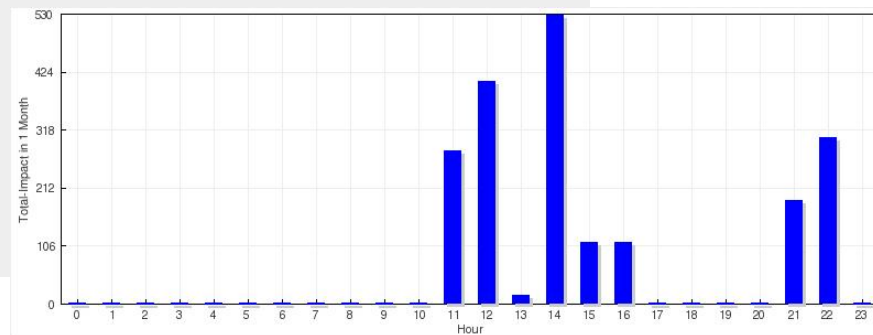
## Count of Actions per Weekday (1 month)



| Weekday | Actions in the past month |      |      |     |      |
|---------|---------------------------|------|------|-----|------|
|         | Log                       | Mail | Kick | Ban | Warn |
| sun     | 0                         | 0    | 0    | 0   | 0    |
| mon     | 0                         | 0    | 0    | 0   | 0    |
| tue     | 26                        | 0    | 0    | 0   | 26   |
| wed     | 0                         | 0    | 0    | 0   | 0    |
| thu     | 0                         | 0    | 0    | 0   | 0    |
| fri     | 0                         | 0    | 0    | 0   | 0    |
| sat     | 0                         | 0    | 0    | 0   | 0    |

| User                 | Total produced Impact in the past month |
|----------------------|---|
| admin (Admin Nutzer) | 1828                                    |
| ::1                  | 114                                     |
| 127.0.0.1            | 8                                       |

## Top-10-Hacker



## Total Impact per Hour (1 month)



# Tests with Apache JMeter



# Apache JMeter Test Plan (I)

- Checks the correct function of detection and reaction by the IDS and IPS system by injecting xss and sql code
  - Variables for the server adress and three moodle testusers
  - Each user handled in one thread



# Apache JMeter Test Plan (II)

- User 1 checks
  - Login
  - Warn user
  - Log attack
  - Kick user
  - Captcha
- User 2 checks
  - Admin mail
  - Ban user
- User 3 checks
  - Total Impact

The screenshot displays the Apache JMeter interface. The main window is titled 'IDS Test Plan.jmx'. The menu bar includes 'Datei', 'Bearbeiten', 'Start', 'Optionen', and 'Hilfe'. The test plan structure is shown on the left, with the following components:

- IDS Test Plan
  - User Defined Variables
  - User\_1
    - HTTP Cookie Manager
    - Login
    - Login OK
    - Response Assertion
    - Warn & Log OK
    - Response Assertion
    - Warn, Log & Kick OK
    - Response Assertion
    - Login
    - Captcha OK
    - Response Assertion
  - User\_2
    - HTTP Cookie Manager
    - Login
    - Warn, Log, Mail & Ban OK
    - Response Assertion
  - User\_3
    - HTTP Cookie Manager
    - Login
    - Loop Controller
    - Totalimpact Count
    - Totalimpact OK
    - Response Assertion
  - View Results Tree

The 'View Results Tree' is expanded on the right, showing a list of test results with green checkmarks indicating success:

- Login
- Login
- Login
- Totalimpact Count
- Login OK
- Warn, Log, Mail & Ban OK
- Totalimpact Count
- Warn & Log OK
- Totalimpact Count
- Warn, Log & Kick OK
- Login
- Totalimpact Count
- Captcha OK
- Totalimpact Count
- Totalimpact OK

The bottom of the window shows a 'Text' field and a 'WorkBench' button.



# Suhosin

- Administration of Suhosin-System
- Statistics of Suhosin-System



# Administration of Suhosin-System (I)

Home ► Site administration ► Suhosin ► Administration

**Navigation**

- Home
  - My home
  - Site pages
  - My profile

**Settings**

- My profile settings
- Site administration
  - Notifications
  - Registration
  - Advanced features
    - Users
    - Courses
    - Grades
    - Location
    - Language
    - Plugins
    - Security
    - Appearance
    - Front page
    - Server
    - Reports
    - Development
    - IDS/IPS
  - Suhosin
    - Administration
    - Filter
    - Encryption
    - Logs

**Suhosin Administration**

**Suhosin System**

Active ☐

Absolute path to logfile

Filter action\*

Filter action redirect

Enable X-Forward ☐

**Executor**

Memory\*

Stackdepth\*

Disable emodifier ☐

Include URL whitelist

Function blacklist

**Eval**

Eval whitelist

Eval blacklist

Disable Eval ☒

**Paths**

Max traversal\*

Activate Symlink ☐

**Misc**

Activate ClamAV ☐



# Administration of Suhosin-System (II)

- The Suhosin-Administration is included as own menu entry
- Administration contains
  - Activate/Deactivate System
  - Filter Reactions
  - Executor-Configuration
  - ClameAV-Configuration
  - APC-Bug
- Filter contains
  - Filter-Configuration for Uploaded Files
  - Filter-Configuration Request Variables
- Encryption
  - Session Encryption
  - Cookie Encryption





# Statistics of Suhosin-System

- Component consists of 2 files:
  - **Logs.php:**
    - Shows an overview of the possible tables
    - Loads the tables from logs\_table.php
  - **Logs\_table.php:**
    - Implements a function which returns a HTML-String with the chosen Table
    - Gets the needed data from the database „mds\_intrusions“



# Analysis

- The basis for the analysis is 1 month (30 days)
- Analysis as following options:
  - Overview
  - Top-10-Hacker
  - Top-10-Targets

| Date/Time           | SIM        | Report      | Reaction      | Attacker  | File      |
|---------------------|------------|-------------|---------------|-----------|-----------|
| 2010-09-09 23:45:10 | SIMULATION | report test | reaction test | 23.0.0.1  | file.php  |
| 2010-09-10 11:26:43 | SIMULATION | report      | reaction      | 127.0.0.1 | index.php |

Example table „Overview“



# OWASP Top 10



# OWASP Top 10 (I)

- **A1: Injection**
  - Secured by IDS/IPS -> input validation
  - Secured by moodle -> input validation
- **A2: Cross-Site Scripting (XSS)**
  - Secured by IDS/IPS -> input validation
  - Secured by moodle -> input validation
- **A3: Broken Authentication and Session Management**
  - Secured by HTTPS-Protocol
- **A4: Insecure Direct Object References**
  - Secured by moodle-user management
- **A5: Cross-Site Request Forgery (CSRF)**
  - not secured -> no unique tokens in links



# OWASP Top 10 (II)

- **A6: Security Misconfiguration**
  - Secured by moodle-security check and detachable error messages  
-> can't be tested, because a part of server configuration (e.g. ports)
- **A7: Insecure Cryptographic Storage**
  - Secured by moodle -> e.g passwords can not be encrypted, hash-coded
- **A8: Failure to Restrict URL Access**
  - Secured by moodle-user management
- **A9: Insufficient Transport Layer Protection**
  - Secured by SSL
  - no cookie encryption by moodle -> Suhosin cookie encryption
- **A10: Unvalidated Redirects and Forwards**
  - must be tested extensively



# For Your Information

- Repository:
  - <http://sourceforge.net/projects/hardeningmoodle/>
- Productive System:
  - <http://websec.mni.fh-giessen.de/moodle>
- Documentation/Wiki (German)
  - <https://wiki.mni.fh-giessen-friedberg.de/index.php/WebSecurity> - Moodle
- Contact
  - Lars-Olof Krause: [hardmoodle@lok-soft.net](mailto:hardmoodle@lok-soft.net)